E-Authentication

Interim Common Credential Assessment Profile

12/19/2003
release 1.3.0

Executive Summary

This document is the Common Credential Assessment Profile. It is part of the Credential Assessment Portfolio as described in the E-Authentication Credential Assessment Framework (CAF). The reader is assumed to be familiar with the CAF. This document contains criteria used to assess all non-PKI based Credential Services (CSs) for use in the E-Authentication initiative. Additional criteria are specified by other profiles.

Release Notes

Interim Release

Document History

Status	Release	Date	Comment	Audience
Released	1.0.0	07/10/03	First Release	Limited
Interim	1.3.0	12/19/03	Released for customer review with the proposal that it be accepted for publication as 2.0.0: • §2 - clarification on scope; • §4.2.2 - inclusion of 'secure channel' criteria to comply with revised NIST SP 800-63; • §4.3.1 - amended criteria to comply with revised NIST SP 800-63; • §4.3.2 - revised to remove implied mutual exclusion; • §4.3.2 - revised to reflect requirements of NIST SP 800-63; • AND minor proofing amendments which have changed neither the semantics nor the intentions of the document. NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.	Customer

Editors

Chris Louden
Kevin Hawkins
Richard G. Wilsher
Dave Silver
Judy Spencer
David Temoshok
Steve Timchak
Von Harrison
Bill Burr
John Cornell
Stephen Sill

Table of Contents

1 INTRODUCTION

This document is part of a suite of documents governing the assessment of credentials for use with the E-Authentication initiative. Please refer to the Interim Credential Assessment Framework (CAF) for an overview. Additional information can be found at http://www.cio.gov/eauthentication/. This profile contains criteria used to assess all non-PKI base Credential Services (CSs). Additional criteria are specified by other profiles.

2 SCOPE

This profile contains requirements to be met by any non-PKI CSs, regardless of the technologies employed.

This profile does not apply to PKI Credential Services. The PKI CAP contains the only applicable criteria for PKI CSs.

Criteria presented in this CAP are cumulative through higher assurance levels. Qualification at any Assurance Level requires validated compliance with all criteria for lower levels of assurance. Assessment at a given Assurance Level also requires validated compliance with multiple profiles; refer to the CAF for more information.

A full description of the role and scope of the CAP documents is contained in the CAF.

3 TERMINOLOGY

This document relies upon terminology established in the E-Authentication Interim CAF, with which the reader is assumed to be familiar.

4 CRITERIA

4.1 Summary

	Level 1	Level 2
Organizational Maturity	□ Established □ Authorization to Operate □ General Disclosure	□ Documentation □ Staffing □ Subcontracts □ Helpdesk □ Audit □ Risk Mgt □ COOP □ Logging □ Configuration Mgt □ Network Security □ Physical Security
Identity Proofing		□ IVP Disclosure □ Records At least one of: □ Confirmed Relationship □ In Person Proofing □ Remote Registration
Authentication Protocol	□ Secure Channel □ Proof of Possession □ Session Authentication □ Stored Secrets □ FIPS Crypto	□ Protected Secrets
Token Strength	□ Uniqueness	
Status Management	□ Credential Validity	□ Credential Status □ Credential Invalidation
Credential Delivery		□ Confirming Delivery

4.2 Assurance Level 1

4.2.1 Organizational Maturity

Tag	Description
Established	1. The CSP shall be a valid legal entity, and a person with legal authority to commit the CSP shall submit the assessment package. 2. The operation system will be assessed as it stands at the time of the assessment. Planned upgrades or modifications will not be considered during the assessment.
Authorization to Operate	1. The CS shall have completed appropriate authorization to operate as required by the CSP policies. 2. The CSP shall demonstrate it understands and complies with any legal requirements incumbent on it in connection to the CS.
General Disclosure	1. The CSP shall make the Terms, Conditions, and Privacy Policy for the CS available to the intended user community. 2. In addition, the CSP shall notify subscribers in a timely and reliable fashion of any changes to the Terms, Conditions, and Privacy Policy.

4.2.2 Authentication Protocol

Tag	Description
Secure Channel	Secrets transmitted across an open network shall be encrypted.
Proof of Possession	The authentication protocol shall prove the claimant has possession and control of the authentication Token (as defined in the CAF).
Session Authentication	Session tokens shall be cryptographically authenticated. For example, session cookies must be encrypted, signed, or contain an HMAC.
Stored Secrets	Secrets such as passwords shall not be stored as plaintext and access to them shall be protected by discretionary access controls that limit access to administrators and applications that require access.
FIPS Crypto	All cryptographic operations shall be done in compliance with FIPS guidance.

4.2.3 Token Strength

Tag	Description
Uniqueness	1. Each subscriber shall self-select at registration time a unique token (e.g., UserID + Password). 2. A user can have more than one token, but a token can only map to one user.

4.2.4 Status Management

Tag	Description
Credential Validity	CS shall maintain record of the status of credentials and not authenticate credentials that have been revoked.

4.3 Assurance Level 2

4.3.1 Organizational Maturity

Tag	Description
Documentation	1. The CSP shall have all security related policies and procedures documented that are required to demonstrate compliance. 2. Undocumented practices will not be considered evidence.
Staffing	1. The CSP shall have sufficient staff to operate the CS according to its policies and procedures. 2. The staff who operate the CS shall have the appropriate skills and abilities for their roles in the operation of the CS.
Subcontracts	1. Any subcontractor or outsourced components of the CS shall have reliable and appropriate contractual arrangements, where the agreement stipulates critical policies and practices that affect the assurance of the CS. 2. Subcontractor responsibilities that are not stipulated in their agreements will not be considered reliable during the assessment.
Helpdesk	A helpdesk shall be available for subscribers to resolve issues related to their credentials during the CSP's regular business hours, minimally from 9am to 5pm Monday through Friday.
Audit	The CSP shall be audited by an independent auditor every 24 months to ensure the organization's practices are consistent with the policies and procedures for the CS. At the time of the assessment, the most recent audit shall have been performed within the last 12 months.
Risk Mgt	The CSP shall demonstrate a risk management methodology that adequately identifies and mitigates risks related to the CS.
COOP	1. The CSP shall have a Continuity of Operations Plan that covers disaster recovery and the resilience of the CS. (Service level agreements are not assessment criteria; they are covered in the licensing arrangements). 2. The CS shall employ failure techniques to ensure system failures do not result in false positive authentication errors.
Logging	The CSP shall log and retain securely for 6 months all significant events related to identity management (e.g., issuance, vetting, revocation).

Tag	Description
Configuration Mgt	The CSP shall demonstrate a Configuration Management methodology that at least includes: 1. Version control for software system components 2. Timely identification and installation of all applicable patches for any software used in the provisioning of the CS.
Network Security	The CSP shall protect their internal communications and systems with measures commensurate with Assurance Level 3 when those communications involve open networks.
Physical Security	The CSP shall employ physical access control mechanisms to ensure access to sensitive areas is restricted to authorized personnel.

4.3.2 Identity Proofing

Tag	Description
IVP Disclosure	The CSP shall publish its identity verification procedures and evidentiary requirements, to the extent necessary to indicate compliance with CAP criteria. That is, the CSP is not de facto required to disclose all of its IVP processes and details. Rather, only enough information to all the Assessment Team to make an informed decision is required.
Records	The CSP shall log and retain securely, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process, which shall, as a minimum, record: Full legal name; Date and place of birth (may not be verified but should be collected); Current address of record. This record shall be retained for the duration of the subscriber account plus at least one year.

For each identity proofing mechanism employed by the CS, one of the following three criteria must be met:

Tag	Description
Confirmed Relationship	1. The CSP shall know the identity of the applicant for at least one of the following significant purposes: a. Employment b. Government program client c. Banking d. Extension of credit of $2,000 or more e. Issuance of insurance f. Regular payment of bills and a duty of the organization to know the true identity of the applicant g. Matriculation at an accredited degree granting educational institution; h. Compliance with public safety, health or other government regulations that impose a duty to verify the identity or members or participants. 2. The CSP shall confirm that the applicant is a person with a current relationship to the organization, record the nature of that relationship (see above) and certify that the relationship is ongoing and in good standing;
In Person Proofing	1. The CSP shall establish the applicant's identity by in-person proofing before the Registration Authority, based on a current government-issued primary photo-ID, such as a driver's license, Military ID or passport. 2. All attributes of the claimed identity must match the attributes in the ID. 3. Attributes of the claimed identity must be attested to by the credential
Remote Registration	To issue or activate the credential, the CSP shall verify the claimed identity via: 1. A credit check that confirms the applicant's name and current address, or phone number (an approved database that binds name and address without requiring the user to input their Social Security Number is acceptable) OR 2. A currently valid credit card or non-prepaid bank card with a billing address that confirms the applicant's address

4.3.3 Authentication Protocol

Tag	Description
Protected Secrets	1. Any secret (e.g., password, PIN, key) involved in authentication shall not be disclosed to third parties. 2. Sharing of secrets with the Agency Application (AA) shall be allowed if no other AA is using the CS. 3. Secrets can be shared with infrastructure elements controlled and designated by GSA (e.g., E-Authentication Service).

4.3.4 Status Management

Tag	Description
Status Responder	CS shall provide, with 95% availability, a secure automated mechanism to allow the E-Authentication Service (according to E-Authentication Service interface specifications) to determine credential status.
Credential Invalidation	CS shall provide a mechanism for a subscriber to disable their credential. The credential should become invalid within 72 hours of the subscriber's request.

4.3.5 Credential Delivery

Tag	Description
Confirming Delivery	The CSP shall issue or renew credentials and tokens in a manner that confirms any one of the applicant's: 1. postal address of record; OR 2. fixed-line telephone number of record.